

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF:
THE HEWLETT PACKARD DESKTOP
COMPUTER LOCATED AT 453 CONCORD
ROAD, FLETCHER, NORTH CAROLINA
28732

Case No. 1:24-mj-45

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, William J. Gang II, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the Hewlett Packard desktop computer (hereinafter "DEVICE"), located at 453 Concord Road, Fletcher, North Carolina 28732, further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI), and, as such, a law enforcement officer of the United States within the meaning of Rule 4 and Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure. I have been employed by the FBI since September of 2007 and have been assigned to the investigation of general criminal matters. I have been charged with the investigation of Federal crimes involving computer intrusions, Internet fraud, wire fraud, bank robberies, extortion, interstate threatening communications, the interstate transportation of stolen property, the sexual exploitation of children and other general criminal

offenses in the Northern District of Ohio and the Western District of North Carolina. At all times during the investigation described in this affidavit, I have acted in an official capacity as a Special Agent of the FBI.

3. I have participated in all the usual methods of investigation, including, but not limited to, physical surveillance, the questioning of witnesses, and the analysis of physical and digital evidence. I have written and executed search warrants, resulting in the seizure of evidence. I have supervised the activities of informants and participated in the execution of consensual monitoring and court ordered Title III wiretaps.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

PROBABLE CAUSE

5. The United States is investigating threatening communications transmitted via email, a violation of 18 U.S.C. § 875(c). A Grand Jury sitting in the Western District of North Carolina indicted JASON ALLEN SPILLARS concerning these threatening communications on June 18, 2024, and the case is now set for trial on December 2, 2024, before the Honorable Max O. Cogburn. 1:24CR44.

6. On or about October 18, 2023, D.J. (hereinafter “VICTIM”) received a message via Facebook from Facebook user “SaintJason Spillars” which read “you are going to be killed.” Facebook user “SaintJason Spillars” had previously posted a picture of VICTIM with a message

which read, in part, “This is my troll: a stupid kike named [D.J.], but we just call him ‘KIKE BOI.’” VICTIM knew the sender of the message to be JASON ALLEN SPILLARS (hereinafter “SPILLARS”), based on previous interactions with SPILLARS and text messages received from SPILLARS in which SPILLARS harassed VICTIM using derogatory African American and Jewish slurs.

7. On or about October 26, 2023, VICTIM received an email message from stpaulustheapostle@gmail.com which read, in part, “I’M GOING TO KILL YOU, DON’T FORGET.”

8. On or about October 29, 2023, VICTIM received an email message from boristhekike@gmail.com with an attached digital picture of the front of VICTIM’s house. A caption below the picture read “are you still living here?”

9. On or about October 30, 2023, VICTIM received an email message from boristhekike@gmail.com which read, in part, “At this point, you have two options: 1. Die... in whatever way is most convenient and simultaneously most rewarding for me. 2. Bow down before me and beg for forgiveness and worship me openly as your Mashiach... and then still be killed for having dared to have been so pathetic in my presence.”

10. Also, on or about October 30, 2023, VICTIM received an email message from boristhekike@gmail.com which read, in part, “you’re going to beg for your life AND I’M GOING TO KILL YOU” and “you think that you have ‘protection’ BUT THEY WILL LAUGH AS I MUTILATE YOU” and “I CAN’T WAIT TO KILL YOU.”

11. Based on the tone and content of the emails sent to VICTIM from stpaulustheapostle@gmail.com and boristhekike@gmail.com, VICTIM knew the sender to be SPILLARS. Thompson Reuters CLEAR, an online aggregate records database, provided SPILLARS' most recent address as 453 Concord Road, Fletcher, North Carolina 28732.

12. On November 13, 2023, this Court authorized an order to Google LLC for records associated with stpaulustheapostle@gmail.com and boristhekike@gmail.com pursuant to 18 U.S.C. § 2703(d). This order was served on Google the same day.

13. On November 15, 2023, Google LLC provided the requested records. A review of the records showed the account boristhekike@gmail.com was only accessed from Internet Protocol (IP) address 97.82.218.86 from October 17 to October 30, 2023. Furthermore, the records showed that on October 26, 2023, the account stpaulustheapostle@gmail.com was also only accessed from IP address 97.82.218.86.

14. On November 28, 2023, a grand jury subpoena was served on Charter Communications requesting subscriber information associated with IP address 97.82.218.86, for the following dates and times:

- a. October 26, 2023, from 22:36:13 GMT to 22:41:53 GMT¹
- b. October 29, 2023, from 18:08:30 GMT to 20:59:56 GMT

¹ GMT is short for Greenwich Mean Time.

c. October 30, 2023, from 00:56:56 GMT to 05:41:20 GMT

15. On February 9, 2024, Charter Communications advised that on the dates and times noted above, IP address 97.82.218.86 was assigned to Kristine Spillars, and provided her address as 453 Concord Road, Fletcher, North Carolina 28732. This address is located within the Western District of North Carolina.

16. On April 25, 2024, and again on November 1, 2024, I interviewed Allen and Kristine Spillars, residents of 453 Concord Road, Fletcher, North Carolina 28732, and parents of SPILLARS. They reported that SPILLARS resided at the 453 Concord Road address beginning sometime at the end of August 2023 and continuing through the period of time the threats were communicated to VICTIM. Allen and Kristine Spillars further advised that SPILLARS used their computer, a Hewlett Packard desktop (the DEVICE), during this time, and that they still currently possess and use the DEVICE as of the filing of this affidavit. On November 5, 2024, Kristine Spillars advised the DEVICE is located in the front room of their home, which they refer to as the “computer room.”

17. On March 22, 2024, Google LLC was served a warrant seeking records associated with stpaulustheapostle@gmail.com and boristhekike@gmail.com. Also on March 22, 2024, Google LLC made the requested records available for secure download from the Google Law Enforcement Request System (LERS). The records were downloaded and reviewed. The records matched and corroborated the complaint made by VICTIM against SPIILLARS.

18. A review of the records associated with stpaulustheapostle@gmail.com also revealed communications between that account and another Gmail account called “heebcock@gmail.com” between October 5, 2023, and October 7, 2023. The email conversation was provided as follows:

*On Sat, Oct 7, 2023, 6:07 PM Aryeh Wold <heebcock@gmail.com> wrote:
I can hear her screams already*

*On Sat, Oct 7, 2023, 6:04 PM Aryeh Wold <heebcock@gmail.com> wrote:
Титус Энни motherfucker²*

On Sat, Oct 7, 2023, 4:11 PM Aryeh Wold <heebcock@gmail.com> wrote:

*On Sat, Oct 7, 2023, 3:46 PM Aryeh Wold <heebcock@gmail.com> wrote:
Я изнасилую и пытаю твою сестру³*

*On Sat, Oct 7, 2023, 3:26 PM Aryeh Wold <heebcock@gmail.com> wrote:
Я убью тебя и всю твою семью⁴*

*On Sat, Oct 7, 2023, 2:39 PM Aryeh Wold <heebcock@gmail.com> wrote:
Bitch boy... Loser. You're a bitch. I'm going to have fun with that girl in the picture. A lot of fun. She might become an overseas sex slave in Russia or somewhere in the eastern block.*

On Sat, Oct 7, 2023, 2:30 PM Aryeh Wold <heebcock@gmail.com> wrote:

² According to Google Translate, “Титус Энни” translates to “Titus Annie”

³ According to Google Translate, “Я изнасилую и пытаю твою сестру” translates to “I will rape and torture yours”

⁴ According to Google Translate, “Я убью тебя и всю твою семью” translates to “I will kill you and your whole family”

Also nigger kike doesn't bother me. It just shows me your lack of wordage and your lack of intelligence. But I know you won't come to Florida on my account. You a pussy. All bark and no bite. You obviously have no idea whom your dealing with. I wish you would come find out. Because it isn't me who will die. It is you and your whole family.

*On Sat, Oct 7, 2023, 2:27 PM Aryeh Wold <heebcock@gmail.com> wrote:
Well come to Florida then tough Guy. Please just do it already so I can put a bullet in your head you faggot. And you seriously have no idea what Z thinks about me. You make shit up. I know better. You better keep your word and be in Florida soon. So I can kill you.*

*On Sat, Oct 7, 2023, 2:19 PM Aryeh Wold <heebcock@gmail.com> wrote:
Bitch boy. Faggot fuck boy chomo loser motherfucker. I'll give you something to laugh at with a pistol in your mouth and have you on your knees. You ain't shit. Just like a mosquito. Annoying asf and needs to be swatted to death. You keep saying that you are going to do something, but you haven't done nothing and you are never going to anything accept watch your family die and watch as you are tortured alive and unalived. I like that girl in the picture. I wonder how many dicks she can take at once before she goes in a coma.*

*On Sat, Oct 7, 2023, 11:05 AM The Pillars <stpaulustheapostle@gmail.com> wrote:
hahahahaha*

*On Sat, Oct 7, 2023 at 11:04 AM The Pillars <stpaulustheapostle@gmail.com> wrote:
I apologize... it's NIGGER KIKE.*

*On Sat, Oct 7, 2023 at 11:04 AM The Pillars <stpaulustheapostle@gmail.com> wrote:
Z thinks of you as a child.*


You're a stupid kike and I will be down in Florida soon.

*On Fri, Oct 6, 2023 at 10:13 PM Aryeh Wold <heebcock@gmail.com> wrote:
You should call your daddy Z and ask him all about Boris korkovdky. You chose the wrong guy to fuck with. You stupid crackhead.*

*On Fri, Oct 6, 2023, 10:11 PM Aryeh Wold <heebcock@gmail.com> wrote:
You don't have much time on this earth
They will be coming for you and those in the picture. You better ask someone about me.
You're fucking with the wrong person and you're going to eat all your words of
emptiness. It's what is known as zietzsche..... hahahaha
Look that up it's Russian fuck boy. That's what will happen to you.*

*On Fri, Oct 6, 2023, 9:28 PM Aryeh Wold <heebcock@gmail.com> wrote:
Thanks for sharing and updating us.....*

*On Fri, Oct 6, 2023, 4:20 PM Aryeh Wold <heebcock@gmail.com> wrote:
And your mom already killed me with that gaping asshole of hers.*

*On Fri, Oct 6, 2023, 4:18 PM Aryeh Wold <heebcock@gmail.com> wrote:

Whatever you say princess*

*On Fri, Oct 6, 2023, 4:17 PM The Pillars <stpaulustheapostle@gmail.com> wrote:
I'm going to kill you.*

*On Thu, Oct 5, 2023 at 11:07 PM Aryeh Wold <heebcock@gmail.com> wrote:
Take your meds psycho boy*

*On Thu, Oct 5, 2023, 11:06 PM Aryeh Wold <heebcock@gmail.com> wrote:
Yeah show them this and all those other one's you sent me. Hey you started something
and now you to pussy boy to finish it. I ain't that little girl and her family. I ain't that little
boy you tried kidnapping at a baseball game. You're a real winner huh boy? Yeah you
thought wrong about me. You wanna keep harassing me and making threats like shit is
funny. Now you scared and threatening with the cops. Hahahaha you soft as fuck. You a
straight up bitch motherfucker. You bitch made. Just like your hero body builder loser
who's dead because he shot up roids. Yeah keep pounding them weights. They ain't
making you any tougher. Awe you going to the cops. Good because they will subpoena*

the phone records, Facebook and all emails and then well you will be locked up. You're going to snitch on yourself. Hahahaha. Loser.

*On Thu, Oct 5, 2023, 10:12 PM Aryeh Wold <heebcock@gmail.com> wrote:
And also if you go to the cops I have all of your texts messages and Facebook messages and emails all saved up just for that. They'll lock you up stupid. You a dumb scared bitch.*

*On Thu, Oct 5, 2023, 10:11 PM Aryeh Wold <heebcock@gmail.com> wrote:
You don't know whether you want to come kill me or call the cops. You confused little boy. Hahahahahaha 🤔🤔🤔🤔🤔🤔🤔🤔🤔🤔🤔🤔🤔🤔🤔🤔*

*On Thu, Oct 5, 2023, 10:09 PM Aryeh Wold <heebcock@gmail.com> wrote:
Lol bitch made motherfucker. You talk all that shit then bitch up like the sissy boy you are. Hahahaha. You are a fucking dick in the booty cracker faggot fuck boy chomo loser. I guess you realized that you played with the wrong person. You pussy boy. I got your mom over here and she taking all this kike dick in her asshole. You're a lame faggot. You mentally challenged little bitch. That's why your dad getting fucked in his ass by niggers. Yeah bitch. You trolled the wrong one fuck boy. You a bitch.*

19. On April 18, 2024, and again on October 28, 2024, VICTIM told me during interviews that heebcock@gmail.com was an email address he had used in the past. He reported that he lost access to this email account in 2021 or 2022, shortly after providing the address to SPILLARS. VICTIM denied sending the messages provided above to SPILLARS.

20. On October 29, 2024, an order pursuant to Title 18 U.S.C. § 2703(d) was served on Google LLC requesting IP log information associated with the email address heebcock@gmail.com.

21. On October 30, 2024, Google LLC responded to the request showing that the account had been deleted on November 5, 2023. IP logs associated with the account were not available.

22. Based on my investigation, there is probable cause to believe that SPILLARS used the DEVICE during the relevant time while he resided with his parents at 453 Concord Road in Fletcher, and that evidence of his activities will be found on the DEVICE.

TECHNICAL TERMS

23. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

24. As described above and in Attachment B, this application seeks permission to search for records that might be found on the DEVICE, in whatever form they are found. One form in which the records might be found is data stored on a DEVICE's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

25. *Probable cause.* I believe those records will be stored on the DEVICE, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer

users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the DEVICE because:

- a. Data on the DEVICE can provide evidence of a file that was once on the DEVICE but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the DEVICE that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the DEVICE that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the

times the DEVICE was in use. The DEVICE file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within the DEVICE may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and

durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password

protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

27. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

29. I submit that this affidavit supports probable cause for a warrant to search the DEVICE described in Attachment A and seize the items described in Attachment B.

Reviewed by Assistant United States Attorney David A. Thorneloe

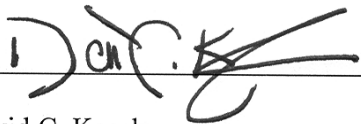
I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Respectfully Submitted,

/S/ William J. Gang II

William J. Gang II
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on November 8, 2024:



David C. Keesler
United States Magistrate Judge



ATTACHMENT A

Property to be searched

The property to be searched is the residence at 453 Concord Road, Fletcher, North Carolina 28732. Within the residence, the property to be searched is a Hewlett Packard desktop computer (the DEVICE).

ATTACHMENT B

Property to be seized

1. A Hewlett Packard desktop computer (the DEVICE).
2. Saved, stored, or contained upon the DEVICE, all records relating to violations of 18 U.S.C. § 875 (c), those violations involving SPILLARS and occurring on and after October 5, 2023, including:
 - a. Records and information relating to the email accounts heebcock@gmail.com, stpaulustheapostle@gmail.com, and boristhekike@gmail.com;
 - b. evidence of who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - c. evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - d. evidence of the lack of such malicious software;

- e. evidence indicating how and when the DEVICE was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the DEVICE user;
- f. evidence indicating the DEVICE user's state of mind as it relates to the crime under investigation;
- g. evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;
- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;
- i. evidence of the times the DEVICE was used;
- j. passwords, encryption keys, and other access devices that may be necessary to access the DEVICE;
- k. documentation and manuals that may be necessary to access the DEVICE or to conduct a forensic examination of the DEVICE;
- l. records of or information about Internet Protocol addresses used by the DEVICE;
- m. records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- n. contextual information necessary to understand the evidence described in this attachment.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.